Известия вузов. Математика
2016, №8, с. 60–68

http://kpfu.ru/science/nauchnye-izdaniya/ivrm/
e-mail: izvuz.matem@kpfu.ru

С.А. ТЮРИН

НЕКОТОРЫЕ СВОЙСТВА ЭЛЕМЕНТОВ ПРОСТОГО ПОЛЯ

Аннотация. Найдены свойства первообразных корней в группах классов вычетов по модулю простого числа, в частности, простых чисел Ферма и простых чисел Софи Жермен, найдены формулы для вычисления произведений элементов в некоторых подмножествах простого поля положительной характеристики.

Ключевые слова: простое поле, простые числа Ферма, простые числа Софи Жермен.

УДК: 511.172

Тематика данной работы возникла при решении задач классификации конечномерных алгебр Ли над полями положительной характеристики. Основополагающей работой здесь является статья А.И. Кострикина и И.Р. Шафаревича [1]. Одним из направлений исследований является изучение строения подалгебр Картана и торов в этих алгебрах Ли, связь между которыми изучалась в разных работах (например, [2]–[5]). Инструментом описания многообразия торов являются группы автоморфизмов алгебр [6], [7]. Возникающие при этом вычисления в конечномерных коммутативных алгебрах над полями положительной характеристики приводят к необходимости решения дифференциальных уравнений, вычисления определителей специального вида, вычисления факториалов элементов простого поля ([8]–[10]).

В данной работе исследуются свойства произведений элементов некоторых подмножеств простого поля положительной характеристики. Основным объектом изучения является мультипликативная группа $G = \mathbb{Z}_p^*$ ненулевых элементов поля классов вычетов $\mathbb{Z}_p$ по модулю нечетного простого числа p. В работе используются понятия, введенные в статье автора [10]. Напомним определения.

Определение 1. Класс вычетов по модулю p будем называть классом 1-го типа, если абсолютно наименьшие вычеты этого класса и обратного по модулю p имеют одинаковые знаки, и классом 2-го типа, если эти знаки разные. Типом целого числа будем называть тип его класса вычетов.

Определение 2. Подмножество $F(a) = \{a, -a, a^{-1}, -a^{-1}\}$ группы $\mathbb{Z}_p^*$ называется четверкой, порожденной элементом $a \in \mathbb{Z}_p^*$.

Четверка является минимальным подмножеством группы $\mathbb{Z}_p^*$, инвариантным относительно операций взятия противоположного и обратного элементов. Все ее элементы имеют одинаковый тип. Он называется типом четверки.

1. Порядки элементов группы $\mathbb{Z}_p^*$

Обозначим через $P(a)$ порядок элемента a в группе $G = \mathbb{Z}_p^*$.

Поступила 13.01.2015

Теорема 1. *При $p = 4n+3$ элементы a и $p-a$ имеют разные порядки в группе $\mathbb{Z}_p^*$ (порядок одного вдвое больше порядка другого).*

Доказательство. Порядки элементов группы $\mathbb{Z}_p^*$ являются делителями числа $p-1 = 4n+2$. Если порядок d элемента a четный: $d = 2k$, где k — делитель нечетного числа $m = \frac{p-1}{2}$, то $a^{2k} \equiv 1 \pmod p$, $a^k \equiv -1 \pmod p$, $(p-a)^k \equiv (-1)^k \cdot a^k \pmod p \equiv 1 \pmod p$. Если же порядок d нечетный, то $a^d \equiv 1 \pmod p$, $(p-a)^d \equiv (-1)^d \cdot a^d \pmod p \equiv -1 \pmod p$, $(p-a)^{2d} \equiv 1 \pmod p$. □

Следствие 1. Пусть $q = 2n+1$ — простое число Софи Жермен, т. е. число $p = 2q+1 = 4n+3$ тоже простое. Тогда во множестве $X = \mathbb{Z}_p^* \setminus \{1, (p-1)\}$ половина элементов является первообразными корнями. Точно так же в этом множестве половина элементов одинакового типа является первообразными корнями.

Доказательство. Порядки элементов группы $\mathbb{Z}_p^*$ являются делителями числа $p-1 = 2q$. Это число имеет четыре делителя: $\{1, 2, q, 2q\}$. Порядок 1 имеет только элемент 1, порядок 2 имеет только элемент $p-1$. Остальные элементы имеют порядки q и $2q$. Количество этих элементов равно $4n$. Они разбиваются на пары $\{a, p-a\}$. В каждой паре один из элементов имеет порядок q, а другой — порядок $2q$, т. е. является первообразным корнем. Внутри каждой пары элементы имеют одинаковый тип. □

Верно и обратное утверждение.

Следствие 2. Пусть число $p = 4n+3$ простое и половина элементов множества $X = \mathbb{Z}_p^* \setminus \{1, (p-1)\}$ является первообразными корнями. Тогда число $q = \frac{p-1}{2}$ — простое число Софи Жермен.

Доказательство. Количество первообразных корней по модулю p равно

$$\varphi(p-1) = \varphi(4n+2) = \varphi(2) \cdot \varphi(2n+1) = \varphi(q).$$

В то же время по условию оно равно половине количества элементов множества X, т. е. $q-1$. Из равенства $\varphi(q) = q-1$ следует, что число q простое. □

Рассмотрим некоторые свойства простого поля классов вычетов по модулю $p = 4n+1$. Группа $G = \mathbb{Z}_p^*$ циклическая порядка $4n$. В ней есть два элемента, порядок которых равен 4. Они являются решениями сравнения $x^2 \equiv -1 \pmod p$. Обозначим через z наименьшее положительное число, удовлетворяющее этому сравнению.

Теорема 2. *Пусть $p = 4n+1$ — простое число, $a \in G$. Тогда*
1) *если число $P(a)$ нечетное, то $P(-a) = 2P(a)$;*
2) *если число $P(a)$ четное, но не делится на 4, то $P(-a) = \frac{1}{2}P(a)$;*
3) *если число $P(a)$ делится на 4, то $P(-a) = P(a)$.*

Доказательство. 1) Пусть $P(a) = k$ — нечетное число. Тогда из $a^k \equiv 1 \pmod p$ следует $(-a)^k \equiv -1 \pmod p$, $(-a)^{2k} \equiv 1 \pmod p$. Отсюда $P(-a)$ делит $2k$. При этом $P(-a)$ не может быть нечетным числом, так как иначе $P(-a)$ делит k, что противоречит соотношению $(-a)^k \equiv -1 \pmod p$. Итак, $P(-a) = 2k_1$, где k_1 — делитель k. Далее, из $(-a)^{2k_1} \equiv 1 \pmod p$ следует $(-a)^{k_1} \equiv -1 \pmod p$, $a^{k_1} \equiv 1 \pmod p$, поэтому k делит k_1. Поскольку k и k_1 делят друг друга, то они совпадают, т. е. $P(-a) = 2P(a)$.

2) Пусть $P(a) = 2k$, где k — нечетное число. Тогда из $a^{2k} \equiv 1 \pmod p$ следует $a^k \equiv -1 \pmod p$, $(-a)^k \equiv 1 \pmod p$, т. е. $P(-a)$ делит k, $P(-a) = k_1$, где k_1 — делитель k. Из

$(-a)^{k_1} \equiv 1 \pmod p$ вытекает $a^{k_1} \equiv -1 \pmod p$, $a^{2k_1} \equiv 1 \pmod p$, т. е. $2k$ делит $2k_1$, k делит k_1. Отсюда $P(-a) = \frac{1}{2}P(a)$.

3) Пусть $P(a) = 4d$. Тогда из $a^{4d} \equiv 1 \pmod p$ следует $(-a)^{4d} \equiv 1 \pmod p$, поэтому $P(-a)$ делит $P(a) = 4d$. Рассмотрим возможные случаи.

Если число $P(-a) = k$ нечетное, то $(-a)^k \equiv 1 \pmod p$, $a^k \equiv -1 \pmod p$, $a^{2k} \equiv 1 \pmod p$. Поэтому $4d$ делит $2k$. Противоречие.

Если $P(-a) = 2k$, где k — нечетное число, то $(-a)^{2k} \equiv 1 \pmod p$, $a^{2k} \equiv 1 \pmod p$. В этом случае также $4d$ делит $2k$. Противоречие.

Если $P(-a) = 4k$, то $(-a)^{4k} \equiv 1 \pmod p$, $a^{4k} \equiv 1 \pmod p$. Поэтому $P(a)$ делит $P(-a)$. Порядки этих элементов делят друг друга, значит, они равны. □

Следствие 1. При $p = 4n + 1$ для любого первообразного корня a число $p - a$ также является первообразным корнем.

Следствие 2. Пусть оба числа n и $p = 4n+1$ простые. Тогда половина элементов множества $\mathbb{Z}_p^* \setminus \{1, z, -1, -z\}$ являются первообразными корнями.

Доказательство. Из условия вытекает, что число n нечетное. Делителями порядка группы $\mathbb{Z}_p^*$ являются числа $\{1, 2, 4, n, 2n, 4n\}$. Все элементы порядков 1, 2 и 4 лежат в подмножестве $\{1, z, -1, -z\}$. Остальные элементы имеют порядки $\{n, 2n, 4n\}$. Их количества равны соответственно $\varphi(n)$, $\varphi(2n) = \varphi(n)$ и $\varphi(4n) = 2\varphi(n)$. Таким образом, половина оставшихся элементов имеет порядок $4n$, т. е. является первообразными корнями. □

Верно и обратное утверждение.

Следствие 3. Пусть число $p = 4n + 1$ простое, и половина элементов множества $\mathbb{Z}_p^* \setminus \{1, z, -1, -z\}$ является первообразными корнями. Тогда число n простое.

Доказательство. Количество первообразных корней равно $\varphi(4n)$. Из условия получается уравнение $\varphi(4n) = 2n - 2$. Если бы число n было четным, то получили бы уравнение $4\varphi(n) = 2n - 2$, что невозможно, так как правая часть не делится на 4. Если же n нечетное, то приходим к уравнению $2\varphi(n) = 2n - 2$, т.е. $\varphi(n) = n - 1$. Это означает, что число n простое. □

Следствие 4. При $p = 4n + 1 > 5$ любой первообразный корень a порождает четверку первообразных корней $\{a, -a, a^{-1}, -a^{-1}\}$. Количество четверок первообразных корней равно

$\varphi(n)$, если число n четное,

$\frac{\varphi(n)}{2}$, если число n нечетное.

Доказательство. Количество первообразных корней равно

$$\varphi(4n) = \begin{cases} 4\varphi(n), & \text{если число } n \text{ четное;} \\ 2\varphi(n), & \text{если число } n \text{ нечетное.} \end{cases}$$

□

Рассмотрим случай простого числа $p = 4n+1$, когда число n не имеет нечетных простых делителей. Тогда оно является степенью числа 2, а число p является простым числом Ферма. Числа Ферма имеют вид $F_m = 2^{2^m} + 1$. Они будут простыми при $m = \overline{0, 4}$. Неизвестно, существуют ли простые числа Ферма при $m > 4$. Простыми числами Ферма вида $p = 4n+1$ будут числа F_m при $m = \overline{1, 4}$. При этом $n = 2^{2^m-2}$. Для простого числа F_m число z имеет вид $z = 2^{2^{m-1}}$.

Таблица 1

m	n	p	z	Количество первообразных корней	Минимальный первообразный корень
1	1	5	2	2	2
2	4	17	4	8	3
3	64	257	16	128	3
4	16384	65537	256	32768	3

Количество первообразных корней по модулю $p = F_m$ равно $\varphi(2^{2^m}) = 2^{2^m-1}$, т. е. половина элементов группы $\mathbb{Z}_p^*$ является первообразными корнями. Это свойство характеризует простые числа Ферма. Именно, справедлива

Теорема 3. *Пусть простое число имеет вид $p = 4n+1$. Если половина элементов группы $\mathbb{Z}_p^*$ представлена первообразными корнями, то p является простым числом Ферма.*

Доказательство. Количество первообразных корней равно $\varphi(4n)$. Получаем уравнение $\varphi(4n) = 2n$. Если число n нечетное, то $\varphi(4n) = 2\varphi(n) = 2n$. Отсюда $\varphi(n) = n$. Поэтому $n = 1$ и $p = 5$. Если число n четное, то $\varphi(4n) = 4\varphi(n) = 2n$. Если каноническое разложение числа n имеет вид $n = 2^m p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, то $\frac{\varphi(n)}{n} = \big(1 - \frac{1}{2}\big)\big(1 - \frac{1}{p_1}\big)\big(1 - \frac{1}{p_2}\big) \dots \big(1 - \frac{1}{p_k}\big)$. В нашем случае $\varphi(n)/n = 1/2$, поэтому $n = 2^m$ и $p = 2^{m+2} + 1$. Число p может быть простым только в том случае, когда $(m + 2)$ является степенью числа 2. □

2. Произведения первообразных корней

Теорема 4. *Произведение всех первообразных корней сравнимо с 1 по модулю p.*

Доказательство. При $p > 3$ первообразные корни входят парами: если g — первообразный корень, то и $g^{-1} \equiv g^{p-2} \pmod p$ тоже является первообразным корнем. Эти два первообразных корня различны. □

Теорема 5. *Пусть $p > 3$ — простое число. Тогда*

a) *произведение всех первообразных корней одинакового типа сравнимо с 1 по модулю p;*

b) *произведение всех первообразных корней первого типа, не превосходящих $(p-1)/2$, сравнимо с 1 по модулю p; аналогично для первообразных корней первого типа, бóльших $(p-1)/2$.*

Доказательство. a) Для всякого первообразного корня обратный по модулю p элемент также является первообразным корнем. Он имеет тот же тип.

b) Для первообразных корней первого типа, не превосходящих $(p-1)/2$, обратный по модулю p элемент также не будет превосходить $(p-1)/2$. Это же справедливо для первообразных корней первого типа, бóльших $(p-1)/2$. □

Замечание. При $p = 5$ первообразных корней первого типа нет.

Теорема 6. *Пусть $p = 4n+1$ и в группе $\mathbb{Z}_p^*$ существуют r четверок второго типа. Тогда*

$$(2n)! \equiv (-1)^r \cdot z \pmod p.$$

Доказательство повторяет обоснование теоремы 2 из [10].

Теорема 7. *Пусть $p = 4n + 1 > 5$ и количество четверок первообразных корней второго типа равно k. Произведение M всех первообразных корней второго типа, не превосходящих $(p-1)/2$, сравнимо с $(-1)^k$: $M \equiv (-1)^k \pmod p$. Аналогично для всех первообразных корней второго типа, бóльших $(p-1)/2$.*

Доказательство. Пусть a — первообразный корень второго типа, не превосходящий $\frac{p-1}{2}$. Он порождает четверку первообразных корней второго типа $\{a, -a, a^{-1}, -a^{-1}\}$. Она разбивается на две пары $\{a, -a^{-1}\}$ и $\{-a, a^{-1}\}$. Элементы первой пары не превосходят $(p-1)/2$, а элементы второй больше $(p-1)/2$. Произведения элементов каждой пары сравнимы с (-1) по модулю p. □

Теорема 8. *Пусть g – первообразный корень по модулю $p = 4n + 1$. Тогда $\operatorname{ind}_g(z)$ может быть равен числу n или $3n$. При этом*

$$\operatorname{ind}_g(z) = n \Leftrightarrow g^n \equiv z \pmod p,$$
$$\operatorname{ind}_g(z)* = 3n \Leftrightarrow g^n \equiv -z \pmod p.$$

Доказательство. Очевидно, $\operatorname{ind}_g(p-1) = (p-1)/2 = 2n$. Из сравнения $z^2 \equiv (p-1) \pmod p$ следует $2\operatorname{ind}_g(z) \equiv 2n \pmod{4n}$. Отсюда получаем $\operatorname{ind}_g(z) \equiv n \pmod{2n}$. Так как величина индекса не превосходит $p-1 = 4n$, то $\operatorname{ind}_g(z)$ может быть равен n или $3n$. Если $\operatorname{ind}_g(z) = n$, то $z \equiv g^n \pmod p$, а если $\operatorname{ind}_g(z) = 3n$, то $z \equiv g^{3n} \pmod p \equiv g^{2n} \cdot g^n \pmod p \equiv -g^n \pmod p$.

Обратно, если $g^n \equiv z \pmod p$, то $\operatorname{ind}_g(z) = n$, а если $g^n \equiv -z \pmod p$, то $g^{3n} \equiv -z^3 \pmod p \equiv z \pmod p$, поэтому $\operatorname{ind}_g(z) = 3n$. □

Теорема 9. *Пусть U — множество первообразных корней, для которых $\operatorname{ind}_g(z) = n$, V — множество первообразных корней, для которых $\operatorname{ind}_g(z) = 3n$. Тогда количество элементов в этих множествах одинаково и равно*

$$2\varphi(n), \quad \text{если число } n \text{ четное};$$
$$\varphi(n), \quad \text{если число } n \text{ нечетное}.$$

Доказательство. Если $n = 1$, то $p = 5$, $z = 2$. Имеется два первообразных корня: 2 и 3. При этом $\operatorname{ind}_2(2) = 1$, $\operatorname{ind}_3(2) = 3$. При $n > 1$ количество первообразных корней кратно 4. Пусть a — первообразный корень. Он порождает четверку первообразных корней $\{a, -a, a^{-1}, -a^{-1}\}$. При четном n числа a и $b = -a$ лежат в одном из множеств U и V, а числа $c = a^{-1}$ и $d = -a^{-1}$ — в другом множестве. Действительно, пусть $\operatorname{ind}_a(z) = t$, где число t равно n или $3n$. Тогда $a^t \equiv z \pmod p$. В этом случае $(-a)^t \equiv (-1)^t \cdot a^t \pmod p \equiv a^t \pmod p$, поскольку число t четное. Это означает, что числа a и b лежат в одном множестве. Аналогично, числа b и d лежат в одном множестве. В то же время числа a и c лежат в разных множествах. Пусть, например, $\operatorname{ind}_a(z) = n$. Тогда $\operatorname{ind}_c(z) = 3n$:

$$c^{3n} \equiv \left(\frac{1}{a}\right)^{3n} \pmod p \equiv \left(\frac{1}{z}\right)^3 \pmod p \equiv (-z)^3 \pmod p \equiv -z^3 \pmod p \equiv z \pmod p.$$

Аналогичные рассуждения показывают, что при нечетном n числа a и d лежат в одном из множеств U и V, а числа b и c — в другом множестве. Общее число первообразных корней по модулю $p = 4n + 1$ равно $\varphi(4n)$, поэтому в каждом из множеств U и V лежит половина этого числа элементов. □

Теорема 10. *Два первообразных корня g и h принадлежат одному и тому же множеству тогда и только тогда, когда $\operatorname{ind}_g(h) \equiv 1 \pmod 4$.*

Доказательство. Заметим, что индекс одного первообразного корня по основанию другого первообразного корня может быть сравним с 1 или 3 по модулю 4. Действительно, если $\mathrm{ind}_g(h) \equiv 0 \pmod 4$, то $h^n \equiv g^{4n} \pmod p \equiv 1 \pmod p$, а если $\mathrm{ind}_g(h) \equiv 2 \pmod 4$, то $h^n \equiv g^{2n} \pmod p \equiv -1 \pmod p$. В обоих случаях число h не является первообразным корнем.

Пусть множества Uи V определены так же, как в теореме 9, и пусть $g, h \in U$. Тогда $\mathrm{ind}_g(z) = \mathrm{ind}_h(z) = n$. Но $\mathrm{ind}_g(h) \cdot \mathrm{ind}_h(z) \equiv \mathrm{ind}_g(z) \pmod{4n}$, т. е. $\mathrm{ind}_g(h) \cdot n \equiv n \pmod{4n}$. Отсюда $\mathrm{ind}_g(h) \equiv 1 \pmod 4$. Аналогично рассматривается случай, когда $g, h \in V$.

Обратно, пусть $\mathrm{ind}_g(h) \equiv 1 \pmod 4$. Если g и h принадлежат разным множествам, например, $g \in U$ и $h \in V$, то $\mathrm{ind}_g(z) = n$ и $\mathrm{ind}_h(z) = 3n$. Из соотношения

$$\mathrm{ind}_g(h) \cdot \mathrm{ind}_h(z) \equiv \mathrm{ind}_g(z) \pmod{4n}$$

получаем $\mathrm{ind}_g(h) \cdot n \equiv 3n \pmod{4n}$, т. е. $\mathrm{ind}_g(h) \equiv 3 \pmod 4$, что приводит к противоречию. □

Теорема 11. *Два первообразных корня g и h принадлежат одному и тому же множеству тогда и только тогда, когда их индексы по любому первообразному корню f сравнимы по модулю* 4.

Доказательство. В силу теоремы 9 выполняется условие $\mathrm{ind}_g(h) \equiv 1 \pmod 4$.

Из соотношения

$$\mathrm{ind}_f(g) \cdot \mathrm{ind}_g(h) \equiv \mathrm{ind}_f(h) \pmod{4n}$$

следует сравнение этих же чисел по модулю 4:

$$\mathrm{ind}_f(g) \cdot \mathrm{ind}_g(h) \equiv \mathrm{ind}_f(h) \pmod 4.$$

Тогда

$$\mathrm{ind}_f(g) \equiv \mathrm{ind}_f(h) \pmod 4. \qquad \square$$

Теорема 12. *Если число n нечетное, то произведения элементов во множествах U и V одинаковы и сравнимы с числом $(-1)^{\varphi(n)/2}$ по модулю p.*

Доказательство. В силу теоремы 9 в каждом из этих множеств вместе с любым элементом a входит элемент $-a^{-1}$. Таким образом, эти множества разбиваются на пары элементов, произведение которых сравнимо с (-1) по модулю p. Число таких пар равно $\varphi(n)/2$. □

В случае четного числа n будем считать, что число p имеет вид $p = 8n+1$. В этом случае множество U состоит из тех первообразных корней, для которых $\mathrm{ind}_g(z) = 2n$, а множество V состоит из тех первообразных корней, для которых $\mathrm{ind}_g(z) = 6n$.

Теорема 13. *Пусть число n имеет $r > 0$ различных нечетных простых делителей.*

1) *Если среди них есть хотя бы одно число, сравнимое с* 1 *по модулю* 4*, то произведения элементов каждого из множеств U и V сравнимы с* 1 *по модулю p.*

2) *Пусть все нечетные простые делители числа n сравнимы с* 3 *по модулю* 4*. Если $r > 1$, то произведения элементов каждого из множеств U и V сравнимы с 1 по модулю p, а если $r = 1$, произведения элементов множеств U и V сравнимы с (-1) по модулю p.*

Доказательство. Пусть g — первообразный корень, принадлежащий множеству U. Индексами первообразных корней по модулю p являются все нечетные числа, не превосходящие $8n$ и взаимно простые с n. Для множества U эти элементы должны быть сравнимы с 1 по модулю 4, а для множества V эти элементы должны быть сравнимы с 3 по модулю 4.

1) Суммы индексов элементов множеств U и V равны $8n\varphi(n)$, если число n нечетное, и $16n\varphi(n)$, если число n четное. Поскольку $g^{8n} \equiv 1 \pmod p$ по определению первообразного корня, то произведения элементов каждого из множеств U и V сравнимы с 1 по модулю p.

2) Сумма индексов элементов множества U равна $8n\varphi(n) - 2^{r+1}n$, если число n нечетное, и $16n\varphi(n) - 2^{r+1}n$, если число n четное. Сумма индексов элементов множества V равна $8n\varphi(n) + 2^{r+1}n$, если число n нечетное, и $16n\varphi(n) + 2^{r+1}n$, если число n четное. Поскольку $g^{4n} \equiv -1 \pmod p$, то при $r = 1$ произведения элементов каждого из множеств U и V сравнимы с (-1) по модулю p, а при $r > 1$ произведения элементов каждого из множеств U и V сравнимы с 1 по модулю p. □

Теорема 14. *Если число p является простым числом Ферма, то*

1) *при $p = 5$ произведение элементов множества U сравнимо с числом z по модулю p, а произведение элементов множества V сравнимо с числом $(-z)$ по модулю p;*

2) *при $p > 5$ произведение элементов множества U сравнимо с числом $(-z)$ по модулю p, а произведение элементов множества V сравнимо с числом z по модулю p.*

Доказательство. Индексами первообразных корней по основанию g являются все нечетные натуральные числа, меньшие 2^{2^m}. Пусть первообразный корень $g \in U$, тогда для любого элемента $a \in U$ будет выполняться условие $\mathrm{ind}_g(a) \equiv 1 \pmod 4$, а для любого элемента $b \in V$ будет выполняться условие $\mathrm{ind}_g(b) \equiv 3 \pmod 4$. Сумма индексов элементов множества U равна $1 + 5 + 9 + \cdots + (4n-3) = (2n-1)n$, а сумма индексов элементов множества V равна $3 + 7 + 11 + \cdots + (4n-1) = (2n+1)n$. Произведение элементов множества U сравнимо с

$$g^{(2n-1)n} \equiv z^{(2n-1)} \pmod p \equiv z^{2n} \cdot \frac{1}{z} \pmod p \equiv (-1)^n \cdot \frac{1}{z} \pmod p \equiv (-1)^{n-1} \cdot z \pmod p.$$

Произведение элементов множества V равно

$$g^{(2n+1)n} \equiv z^{(2n+1)} \pmod p \equiv z^{2n} \cdot z \pmod p \equiv (-1)^n \cdot z \pmod p.$$

Если $p = 5$, то $n = 1$, $z = 2$, $U = \{2\}$, $V = \{3\}$. В этом случае произведение элементов множества U сравнимо с числом z по модулю 5, а произведение элементов множества V сравнимо с числом $-z \equiv 3 \pmod 5$.

В остальных случаях число n будет четным, поэтому произведение элементов множества U сравнимо с числом $(-z)$ по модулю p, а произведение элементов множества V сравнимо с числом z по модулю p. □

Группа $\mathbb{Z}_p^*$ имеет подгруппу четвертого порядка $\{1, z, -1, -z\}$. Отображение $a \to a^n$ является сюръективным гомоморфизмом группы $\mathbb{Z}_p^*$ на эту подгруппу.

Теорема 15. *Пусть $a \in \mathbb{Z}_p^*$. Тогда*

$$a^n \equiv \begin{cases} \pm 1 \pmod p, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ \pm z \pmod p, & \text{если } a \text{ — квадратичный невычет по модулю } p. \end{cases}$$

Доказательство.

$$(a^n)^2 = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p = \begin{cases} +1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p. \end{cases}$$

Теорема 16. *Пусть X — множество всех элементов группы $\mathbb{Z}_p^*$, удовлетворяющих условию $a^n \equiv z \pmod p$, Y — множество всех элементов группы $\mathbb{Z}_p^*$, удовлетворяющих условию $a^n \equiv -z \pmod p$. Тогда*

1) *количество элементов в этих множествах одинаково и равно n;*

Таблица 2

d	m	h	Π	Π_k
2	$2n$	-1	$\Pi \equiv -1 \pmod p$	$\Pi_k \equiv -g^{2k} \pmod p,\ k = 1, 2, ..., 2n-1$
4	n	z	$\Pi \equiv -1 \pmod p$	$\Pi_k \equiv -g^{4k} \pmod p,\ k = 1, 2, ..., n-1$
n	4	g^4	$\Pi \equiv (-1)^{n-1} \pmod p$	$\Pi_1 \equiv (-1)^{n-1} \cdot z \pmod p$ $\Pi_2 \equiv (-1)^n \pmod p$ $\Pi_3 \equiv (-1)^n \cdot z \pmod p$
$2n$	2	g^2	$\Pi \equiv -1 \pmod p$	$\Pi_1 \equiv 1 \pmod p$

2) *произведение K элементов множества X сравнимо с $(-1)^{n+1} \cdot z \pmod p$, произведение M элементов множества Y сравнимо с $(-1)^n \cdot z \pmod p$.*

Доказательство. Выберем первообразный корень g, удовлетворяющий условию $g^n \equiv z \pmod p$, и возьмем элемент $h = g^4$. Он удовлетворяет условию $h^n \equiv 1 \pmod p$ и порождает подгруппу $H = \{1, h, h^2, \ldots, h^{n-1}\}$ в группе $G = \mathbb{Z}_p^*$. Множества X и Y являются смежными классами этой подгруппы:

$$X = gH = \{g, g^5, g^9, \ldots, g^{4n-3}\},$$
$$Y = g^3H = \{g^3, g^7, g^{11}, \ldots, g^{4n-1}\},$$
$$K = g^{1+5+\cdots+(4n-3)} = g^{n(2n-1)} \equiv z^{2n-1} \pmod p \equiv \frac{(-1)^n}{z} \pmod p \equiv (-1)^{n+1} z \pmod p,$$
$$M = g^{3+7+\cdots+(4n-1)} = g^{n(2n+1)} \equiv z^{2n+1} \pmod p \equiv (-1)^n z \pmod p. \qquad \square$$

Группа $G = \mathbb{Z}_p^*$ циклическая порядка $4n$. Каждому делителю d числа $4n$ соответствует подгруппа H порядка d. Пусть g — первообразный корень по модулю p. Образующим элементом подгруппы H является $h = g^m$, где $m = \frac{4n}{d}$: $H = \{1, h, h^2, \ldots, h^{d-1}\}$. Найдем произведения элементов подгруппы H, а также элементов смежных классов по этой подгруппе

$$\prod = \prod_{i=0}^{d-1} h^i = h^{\frac{d(d-1)}{2}} = g^{2n(d-1)} \equiv (-1)^{d-1} \pmod p.$$

Для смежного класса aH, где $a = g^k$ $(k = 1, 2, \ldots, m-1)$, произведение элементов равно

$$\prod_k = \prod_{i=0}^{d-1} (ah)^i = (-1)^{d-1} \cdot a^d \equiv (-1)^{d-1} \cdot g^{dk} \pmod p.$$

Рассмотрим некоторые примеры. Будем для определенности считать, что $\mathrm{ind}_g(z) = n$.

Теорема 17. *Пусть $p = 4n + 3$ — простое число, g – первообразный корень по модулю p, U — множество первообразных корней, удовлетворяющих условию $\mathrm{ind}_g(h) \equiv 1 \pmod 4$, V — множество первообразных корней, удовлетворяющих условию $\mathrm{ind}_g(h) \equiv 3 \pmod 4$. Тогда для каждого из множеств U и V произведение всех его элементов сравнимо с 1 по модулю p.*

Доказательство. Множества U и V вместе с каждым своим элементом содержат и обратный элемент. Если $\mathrm{ind}_g(a) = x$ и $b = \left(\frac{1}{a}\right) \pmod p$, то $\mathrm{ind}_g(b) = p - 1 - x$. Нечетные числа x и $(p - 1 - x)$ имеют одинаковые остатки при делении на 4. $\square$

Литература

[1] Кострикин А.И., Шафаревич И.Р. *Градуированные алгебры Ли конечной характеристики*, Изв. АН СССР. Сер. матем. **33** (2), 251–322 (1969).
[2] Демушкин С.П. *Подалгебры Картана простых неклассических p-алгебр Ли,* Изв. АН СССР. Сер. матем. **36** (4), 915–932 (1972).
[3] Wilson R.L. *Cartan subalgebras and tori in prime characteristic*, Proc. Amer. Math. Soc. **53**, (2), 325–327 (1975).
[4] Тюрин С.А. *О подалгебрах Картана общей алгебры Ли картановского типа*, Матем. сб. **116** (4), 547–557 (1981).
[5] Barnes D.W. *On Cartan subalgebras of Lie algebras*, Math. Z. **101**, 350–355 (1967).
[6] Wilson R.L. *Automorphisms of graded Lie algebras of Cartan type*, Comm. Algebra, **3**, № 7, 591–613 (1975).
[7] Тюрин С.А. *Классификация торов в алгебре Цассенхауза*, Изв. вузов. Матем., № 2, 69–76 (1998).
[8] Тюрин С.А. *Некоторые типы дифференциальных уравнений над полем конечной характеристики*, Изв. вузов. Матем., № 1, 81–83 (1992).
[9] Тюрин С.А. *Модулярная тригонометрия*, Нелинейный мир, **6** (11–12), 704–712 (2008).
[10] Тюрин С.А. *Символ типа и теорема Вильсона*, Изв. вузов. Матем., № 9, 47–53 (2012).

С.А. Тюрин

Нижегородский государственный университет им. Н.И. Лобачевского,
пр. Гагарина, д. 23, г. Нижний Новгород, 603950, Россия,

e-mail: saturin@list.ru

S.A. Tyurin

Some properties of elements of the prime field

Abstract. We obtain some properties of primitive roots in the groups of residue class modulo prime number, in particular, Fermat primes and Sophie Germain primes. We also obtain some formulas for computation of products of elements in some subsets of the prime field of positive characteristic.

Keywords: prime field, Fermat primes, Sophie Germain primes.

S.A. Tyurin

Lobachevsky State University of Nizhni Novgorod,
23 Gagarin Ave., Nizhni Novgorod, 603950 Russia,

e-mail: saturin@list.ru